3Com® Switch 4050 and 4060 Gigabit Multilayer Switching Software Version 3.05 Release Notes

Table of Contents

Related Documentation

Software License Agreement

About This Software Version

Upgrading to Software Version 3.05

Fixes for Known Faults

Points to Note when using the Switch 4050 and 4060

- Supported Expansion Modules
- Inserting and Replacing Expansion Modules
- Auto-MDIX
- Serial Cable
- TFTP Upgrades
- Configuring Link Aggregations
- LACP Protocol
- CD-ROM
- Telnet and HyperTerminal
- Software Update Utility
- SLIP
- Traceroute
- QoS

Software Upgrade

IGMP

XRN Distributed Fabric

Long Haul Fiber GBICs

WinSock 2 Libraries for Windows 95

Known Problems

Known Interoperability Issues

Software Upgrades

How do I upgrade the Software on my Switch?

3Com Network Supervisor

Documentation Errors and Omissions

Management Interface Reference Guide (DHA1770-9AAA03):

3Com Switch 4050 and 4060 Getting Started Guide (DUA1770-9AAA04)

3Com Switch 4050 and 4060 Implementation Guide (DUA1770-9BAA03)

Related Documentation

Please use these notes in conjunction with the following documents:

- “3Com Switch 4050 and 4060 Series Getting Started Guide”
  Part number: DUA1770-9AAA03 (supplied with your SuperStack 3 Switch and in PDF format on the 3Com Web site)
- “3Com Switch 4050 and 4060 Implementation Guide”
  Part number: DUA1770-9BAA03 (supplied in PDF format on the CD-ROM that accompanies your Switch and on the 3Com Web site)
- “3Com Switch 4050 and 4060 Management Quick Reference Guide”
  Part number: DQA1770-9AAA03 (supplied with your SuperStack 3 Switch and in PDF format on the 3Com Web site)
- “3Com Switch 4050 and 4060 Management Interface Reference Guide”
  Part number: DHA1770-9AAA03 (supplied in HTML format on the CD-ROM that accompanies your Switch and on the 3Com Web site)

You can obtain the latest technical information for your Switch, including a list of known problems and solutions, from the 3Com Knowledgebase:

http://knowledgebase.3com.com

Software License Agreement

Before you use the 3Com Switch 4050 and 4060 software, please ensure that you read the license agreement text. You can find the license.txt file on the CD-ROM that accompanies your product, or in the self-extracting exe that you have downloaded from the 3Com website.

If you intend to use a 3Com Switch 4050 and 4060 with version 3.05 software in a Distributed Fabric, ensure that all other units in the Distributed Fabric are upgraded to version 3.05 as well. 3Com cannot guarantee correct operation if different software versions are used within a Distributed Fabric. Please note that under the terms and conditions of the 3Com End User Software License Agreement, you will need to purchase a service contract for each existing 3Com Switch 4050 and 4060 before upgrading to version 3.05 software.

About This Software Version

The version 3.05 agent feature set is a compatible superset of that provided by all previous versions of this software. This software provides support for the following:

- 3Com Switch 4050 (3C17708)
- 3Com Switch 4060 (3C17709)

The 3Com Switch 4050 and 4060 Gigabit Multilayer Switching Software Version 3.05 does not operate on any other 3Com Switch.

Upgrading to Software Version 3.05

3Com strongly recommends that you upgrade all Switch 4050 and 4060 units which are running a previous version of software to version 3.05.

Fixes for Known Faults

The following known faults have been fixed in version 3.05:

- When a group of routers that exchange RIP messages use DHCP/BOOTP for the configuration of the first IP interface and receive IP addresses within the same network, the first router to get its configuration can interfere with the other routers from getting their configuration. You should disable RIP until the DHCP/BOOTP/ process completes.
- When upgrading from any previous version of software to V3.00 the discard on Tx setting was corrupted for link aggregations. The effect of this could possibly result in traffic being blocked due to oversubscribed 10/100M links. Upgrading to version 3.05 will correct this problem and force Discard on transmit to 'on' for link aggregations.
- Under some circumstances with high traffic loads it was possible that on a fabric merge, one or both of the XRN units could reset.

- Some packet duplication lasting for a few seconds was possible after an XRN fabric split.
- TCP connection setups could corrupt the memory causing the Switch to reset. This has been seen whilst managing the unit via the Web interface, with the http traffic going via a proxy server hosted by Novell Border Manager.
- Using the Web Interface, the 1hour statistics and the 24hour statistics were the same.
- Excessive and/or inconsistant failover times on XRN Fabric split and merge were found under some configurations and traffic scenarios.

Points to Note when using the Switch 4050 and 4060

Supported Expansion Modules

- 3C17710 – 4 port 1000BASE-SX module
- 3C17711 – 4 port 1000BASE-T module
- 3C17712 – 4 port 1000BASE-LX module
- 3C17714 – 4 port GBIC module
- 3C17716 – XRN Interconnect module

Inserting and Replacing Expansion Modules

CAUTION: *The Modules are not hot-insertable or hot-swappable. You must always power down the Switch and disconnect it from the mains before installing or removing a Module.*

- When you insert a Module into the Switch, push the Module in until the Module's back plate is in full contact with the Switch's chassis.
- When you have inserted the Module, secure the Module to the Switch by tightening the three cap-tive screws fully with a screwdriver.
- If an error is indicated during the Power On Self Test, check that the module has been correctly inserted.
- Ensure that the blanking plate and its fastenings are stored in a suitable place. If the module is removed, the blanking plate must be replaced.
- When an expansion module is replaced by another module of a different type, the configuration will not be completely reset to factory defaults. Specifically, the following module parameters will not be reset:
    - Static addresses
    - Resilient links
    - IGMP router ports
    - RMON alarm variables
    - Spanning Tree port data
- It is recommended that all module configuration should be reviewed after the expansion module has been replaced.

Auto-MDIX

Auto-MDIX is not available if auto-negotiation is disabled on a port. That port will only operate in MDIX mode.

Serial Cable

When using a serial cable you must ensure that it is wired correctly as described in Appendix B of the Getting Started Guide.

TFTP Upgrades

Note that when initiating a TFTP upgrade using the Web interface or CLI, if an incorrect TFTP server IP address or software upgrade filename is entered you will not be able to correct the IP address or filename until the TFTP upgrade operation has timed out. The default time out period is 5 minutes.

You can avoid the 5 minute time out period by aborting the upgrade, either using the *Abort* button in the Web interface or the *Esc* character in the Command Line Interface.

Configuring Link Aggregations

When creating a manual aggregation between two systems the ports in the aggregation must not be physically connected together until the aggregation has been correctly configured at both ends of the link. Failure to configure the aggregation at both ends before physically connecting the ports can result in a number of serious network issues such as lost packets and network loops.

LACP Protocol

CAUTION: *The LACP protocol is disabled by default in version 3.05 software. Some legacy devices do not support LACP and 3Com strongly recommends LACP remains disabled on ports connected to these devices (in rare cases, if LACP is enabled on ports connected to these devices, it can result in incorrect network configurations).*

CD-ROM

When using the setup.exe that displays the splash screen on the CD-ROM you may experience a problem if you have an early version of virus checker installed on your PC. If you experience this problem the following error is displayed when the `setup.exe` is activated:

```
Application Error

Exception EResNotFound in

Module 0DSCD.EXE at 0016:0B37

Resource TMainForm not found.
```

You can either:

- Turn off your virus checking software whilst using the CD-ROM

or

- Upgrade your virus checking software to the latest version.

Telnet and HyperTerminal

Accessing the Command Line Interface via Telnet or Windows HyperTerminal using TCP/IP may not work correctly on some platforms unless it has been configured to send line feeds with carriage returns. To set this for Telnet enter **`set crlf`** when in command mode. To set this for HyperTerminal click on the *Settings* tab in the *Properties* screen, click *ASCII Setup..* and ensure that *Send line ends with line feeds* is checked within the *ASCII Sending* section.

You should not configure HyperTerminal in the above way if you are using a console cable to make a direct connection to the Switch.

Software Update Utility

The Software Update Utility (SUU) is a Windows application used to serially update the software to the Switch via the console port. The preferred method for updating the software on the Switch is via a TFTP upgrade. The SUU should only be used if a TFTP upgrade has failed. This utility is available on the CD-ROM that accompanies your Switch.

SLIP

The SLIP interface can only be accessed though the console port on unit1, the console port on other units can not access this interface.

Traceroute

Traceroute implementation is using UDP probe packets to perform the traceroute operation. MS-DOS or PC-DOS systems have a Non-Standard implementation of TCP/IP, which may cause them to not respond to the Traceroute UDP probe packets.

QoS

If you have configured QoS on a single unit (such as the SuperStack 3 Switch 4924, 4950, or the 3Com Switch 40x0) and it merges with a unit having fewer QoS capabilities (Switch 4900 and 4900 SX) to create a mixed Distributed Fabric, some of the user configured settings may be lost. 3Com recommends configuring QoS after the Distributed Fabric has been created.

Software Upgrade

If you start a software upgrade using the CLI or a web browser, the switch will report the status of each unit as it finishes its upgrade. If you are upgrading a Distributed Fabric and use the web, or connect to the CLI using telnet, and your computer is directly connected to a port on the Distributed Fabric, the connection will break when the unit with that port completes its upgrade and restarts. If there are other units still to upgrade at this point, you will not get status reports about them, but the upgrade should continue normally. You can check this by using the **`system summary`** command on each unit and verifying that the Operational Version shows the correct version of software. Note that this problem will not occur if your computer is connected indirectly via a hub, a router, or another switch that is not part of the Fabric.

IGMP

- IGMP querying is disabled by default due to potential interoperability issues with core products that do not follow the lowest IP address election method. Refer to Chapter 3 “Using Multicast Filtering” of the Implementation Guide for more information about this method.
- If you wish to run multicast sessions in a network that does not contain any IGMP routers (or queriers), you can configure the Switch to automatically negotiate with compatible devices on VLAN 1 to become the querier. Use the **`bridge multicastFilter igmp queryMode`** CLI command. The Switch 4050/4060 is compatible with any device that conforms to the IGMP v2 protocol.
- If IGMP snooping is enabled then IP multicasts will only be forwarded within a VLAN if an IGMP querier is present in that VLAN.

XRN Distributed Fabric

- If the XRN Interconnect breaks or is disconnected, all router interfaces in one of the units (including the management interface if it was set manually) will go to the DOWN state. The interfaces will stay down as long as the unit detects another unit with the same interfaces. Even if the management interface is modified it will stay in the DOWN state. If the management interface was set by AutoIP, then one unit will shut down all interfaces, but the management interface will acquire a new IP address via the AutoIP process.
- To ensure maximum security after connecting units in a Distributed Fabric, and the units have reconfigured themselves, 3Com recommends that you reconfigure the user names and passwords defined in the local database using the *Security* > *User* web operation or the **`system management password`** CLI command. This recommendation is not necessary if you are using a RADIUS authentication server on your network to validate management access to the units.
- To provide support for XRN's Distributed Resilient Routing, XRN-enabled Switches send periodic (once a second) ARP based broadcasts on the VLAN associated with the first non-default IP interface defined on the fabric. This is typically, but not always, interface 3. This protocol will also occur on a single Switch fabric as long as it has at least one non-default interface. These broadcasts will not impact network performance.

Long Haul Fiber GBICs

- It is possible to enable pause mode flow control for Long Haul Fiber GBIC's using the Web interface *Physical Interface* > *Ethernet* > *Setup* operation and changing the Default Full Duplex Flow control to *Enabled*, or by using the CLI **`physical interface ethernet flowControl`** command and entering **on**. However, pause flow control does not work correctly on Long Haul fiber due to packet propagation delays over the long distances involved and therefore this form of flow control should not be used.

WinSock 2 Libraries for Windows 95

Microsoft WinSock 2 is an application that helps other applications talk to other computers and devices on networks and the Internet.

Microsoft Windows 98, Microsoft Windows NT 4 and Microsoft Windows 2000 already have this application installed, so if you use these operating systems, you will not need to install WinSock 2 on your machine.

If you use Windows 95, you may need to install this. Early versions of Windows 95 did not

include this, while later versions did. If your system requires WinSock 2 you can locate this application in the "Software and Utilities section" of the CD-ROM that accompanies your Switch.

Known Problems

- 3Com recommends that link aggregations should not be configured with a mixture of automatic and manual member ports. In addition, 3Com recommends that LACP is disabled on ports that are added manually to aggregations. Otherwise:
    - If the port is initially unconnected when it is manually added to an aggregation: LACP may unexpectedly move the port to another aggregation when the port is subsequently connected to a partner device.
    - If the port is initially connected to another LACP enabled partner device: The LACP partnerId of the device may conflict with that of the manual aggregation and cause a CLI error message to be generated.

If an automatic aggregated link (created by LACP) contains ports with different VLAN membership, the aggregated link will inherit the VLAN membership of the first port that comes up in the aggregated link. It will override any pre-defined VLAN membership for the aggregated link.

- 3Com recommends that you set individual ports that are to be members of an aggregated link to the same VLAN membership. This ensures communication between all VLANs at all times.
- When or if you should decide to downgrade to an older version of the agent software, you may notice inaccurate information displayed within the web browser interface. This is typically seen as inactive hotspots in the interface. If this should occur, 3Com recommends that you exit the browser, clear the browser cache, and begin another session.
- If in the Distributed Fabric the user defines the management interface only (is used as a Switch), when the Distributed Fabric is split both units will continue to use the same IP address for management. This can make the units management interface unreachable until the IP address is changed on one of the units. 3Com recommends that in this case the management interface be set to auto configure.
- On downgrade to an earlier agent version (e.g. 2.00) any QoS configuration created before the downgrade will be lost. However, if a QoS configuration was created originally on 2.00, and no additional QoS configuration have been made with the 3.05 agent, then on downgrade the original QoS configuration will still exist on 2.00.
- In a Layer-2 only network (i.e. with no Multicast Routers) multicast traffic destinations may not be learnt for up to 5 minutes after a switch is powered on, or is reset.
- The Switch does not display an error message if inappropriate, but otherwise legal, IP addresses are used for certain configurations. For example, the IP address of the switch can be supplied as the tftp server address for software upgrade. No error is displayed to warn of the mistake. The solution is to supply a more appropriate IP address.
- The **`system management password`** CLI command should not be used when logged in as a user authenticated via RADIUS. To change a password in the local (non-RADIUS) database, use the **`security device user modify`** CLI command.
- The spanning tree mode is not synchronised between units following a Distributed Fabric merge. This should not cause any problems for the network since rapid spanning tree is fully backward compatible with legacy spanning tree. Where units within the Distributed Fabric are operating in different spanning tree modes, the user interfaces are not capable of reflecting this – they will choose one setting or the other when asked to show the current spanning tree mode. When a new spanning tree mode is written to the Distributed Fabric (via any of the user interfaces), this will be set on all units within the Distributed Fabric regardless of whether the spanning tree mode previously

differed from unit to unit.

- Half-duplex flow control (backjamming) cannot be enabled or disabled on a per port basis. If any port on a specific unit is reconfigured, all half-duplex ports on that unit will be changed to the new configuration.
- When setting up a SLIP IP address and an IP address for the unit you must ensure that the assigned IP addresses are different.
- The default set-up for Netscape 4.76 on Solaris 2.6 may cause problems when using *System > Telnet > Connect*. By changing the application that Netscape launches from 'xterm' to 'dtterm' the problem is overcome. This is accomplished as follows:

  1. From the *Edit* menu in Communicator, select *Preferences*.

  2. Click the arrow next to *Navigator* to expand its sub-menu and select *Applications*.

  3. In the *Applications* list in the right-hand pane, click on the row that has telnet in the *Description* column and click the *Edit* button.

  4. In the *Edit* window, the text in the *Application*: box should be changed from:

     ```
     xterm -e telnet %h %p
     ```

     to

     ```
     dtterm -e telnet %h %p
     ```

  5. Click *OK* to close the *Edit* window and click *OK* to close the Preferences window. *System->Telnet->Connect* should now connect correctly with the device.

- Netscape 4.7x browsers may crash if the browser window is maximised or re-sized whilst loading switch management screens.
- If while using Netscape with the Web management interface, you attempt to access an area which is restricted due to your current access level, you may be prompted repeatedly for a username and password. To get out of this situation, click OK when you are asked if you want to reauthenticate, then click *Cancel* on the username and password entry box. A message stating *"401 Unauthorized"* will be displayed. You may now log in to the Web management interface again. To avoid this, log in using a higher access level, or do not attempt to access areas of the Web interface which are restricted for your access level.
- When using Netscape 4.7 it is recommended not to open multiple browsers and then visit other Web sites before returning to the 3Com web management page. Scripts loaded by other web sites can overwrite the settings required by the 3Com web management.
- If Netscape is being used to log into the device via the Web interface, and all attempts to the RADIUS server time out, the next authentication attempt may fail immediately. To avoid this, wait several seconds before retrying the authentication attempt.
- If you use Netscape to manage your Switch you may experience problems when trying to change the user password.

  3Com recommends that if you use Netscape and you need to change the password you do so via the CLI command. To do this from the Web interface Device View, use the System > Telnet > Connect operation to start a Telnet connection and then use the `security device user modify` CLI command.

- If the error, *The previous command window is still active* is displayed when using the Web interface, you must close that window before you can select another operation. You should then press *Reload* (Netscape) or *Refresh* (Internet Explorer) in your Web browser.
- When performing a software upgrade via the *System->Control->Software Upgrade* Web interface, the *OK* and *Cancel* buttons may be partially obscured by the edge of the window. This issue only occurs when all of the following conditions exist:
    - Windows 95
    - IE5.0 or IE5.5
    - Screen resolution set to 800x600.
    - Java plugin version earlier than 1.3.1

  This problem can be fixed by upgrading to Java plugin version 1.3.1 or later via the following link.

  http://java.sun.com/getjava/download.html

- The 3Com Switch 4050 and 4060 Web interface can only be accessed by any of the following Web browsers:
    - Microsoft Internet Explorer v5.0
    - Microsoft Internet Explorer v5.5
    - Microsoft Internet Explorer v6.0
    - Netscape Communicator v4.76
    - Netscape Communicator v6.2
- The 3Com Switch 4050 and 4060 Web interface can be accessed on any of the following PC operating systems:
    - Microsoft Windows 95
    - Microsoft Windows 98
    - Microsoft Windows NT v4.0
    - Microsoft Windows 2000
    - Microsoft Windows XP
    - Solaris 2.6
- Do not disable IGMP snooping on the unit when there are hosts in the segments subscribing to multicast IP groups. Hosts may be unable to re-subscribe to the same multicast IP group, for more than 5 minutes, or until the unit is re-booted.
- Pause packets are counted incorrectly. Received pause packets are included in the transmit packet counters. Transmitted pause packets are included in the receive packet and octet counters.
- If a port is being blocked by Spanning Tree Protocol (STP), and STP is disabled, then the port remains blocked until the Switch is reset.
- Internet Explorer 5 - If *'Ignore font styles specified on Web Pages'* or *'Ignore font sizes specified on Web Pages'* are selected, then the appearance of the web interface will be unpredictable. 3Com recommends that neither of these tools are selected (options are found under Internet Explorer 5 menu *Tools* > *Internet Options* > *Accessibility* > *Formatting*).
- BOOTP address does not renew after 1 hour. The IP address is dropped and replaced with 0.0.0.0. The IP address is lost for only a few minutes every hour but is re-established.
- In the v2.52 release and above, Spanning Tree is enabled by default.
- If you should decide to downgrade to an older version of the agent software, you may notice inaccurate information displayed within the web browser interface. This is typically seen as inactive hotspots in the interface. If this should occur, 3Com recommends that you exit the browser, clear the browser cache, and begin another session.
- If you have a QoS profile applied to a port with a service level that remarks the DSCP field, then all the incoming traffic will be remarked. Traffic which is identified by the service level profile will be marked accordingly. Traffic that does not match the service level profile will be remarked with a DSCP value of 0 (best effort). The effect of this is that traffic which identified as “no mark” will be

remarked. To avoid this, we recommend that you do not mix "*DSCP marking"* and *"DSCP No-change"* service levels.

- 802.1p (packet prioritization) overwriting. If the ingress port is untagged and the egress port is tagged, the packet's 802.1p priority will be marked appropriately. However, if the ingress port is tagged and the egress port is tagged, the packet's 802.1p priority will not be remarked.
- DSCP value of 0 cannot be used as a QoS classifier.
- Ethertype IP (0x800) and ARP (0x806) cannot be used as QoS classifiers.
- The *OK* button in the *System* > *Cache Config* > *Summary* of the web interface does not function properly if you have Windows 95 loaded and are using Internet Explorer version 5.5. The status may change while the summary screen is open and therefore reflect an inaccurate reading.
- If Spanning Tree is disabled on your Switch, you must have each port assigned to an untagged VLAN. Ports can also be assigned to multiple tagged VLANs.
- Using the Web interface operation *Physical Interface* > *Ethernet* > *Setup*, it is not possible to disable a range of ports if the port types included in the range are different (for example, fiber and copper). The CLI command **`physicalInterface Ethernet Portstate`** must be used instead. The CLI also must be used to disable an Empty GBIC port.
- You may see addresses in the RIP Neighbors table that do not belong to any of your locally configured subnets. This will not cause any negative effects to routing while using RIP.
- It is not possible to access the Device View in the Web interface if the Switches in your Distributed Fabric are running different versions of the Gigabit Multilayer Switching software.
- When upgrading the Gigabit Multilayer Switching software within a Distributed Fabric containing both SuperStack 3 Switch 4900 Family and 3Com Switch 40x0 Family units via the Web interface, it is necessary to enter both software file names on the same line in the Filename text box, separated by a space (e.g. gmi3_05.bin s3g3_05.bin). Failure to do so may result in a mixed software version Distributed Fabric and loss of connection to the Web interface.

Known Interoperability Issues

An incompatibility exists in the default settings for Link Aggregation between the Switch and the following 3Com products:

- 3Com Switch 4007
- SuperStack II Switch 3900
- SuperStack II Switch 9300
- CoreBuilder 9000 family
- CoreBuilder 9400
- CoreBuilder 3500

The products listed above disable auto-negotiation when a port is added to an aggregated link (trunk).

In order for link aggregation (trunking) to work, ports at either end of an aggregated link (trunk) must be identically configured. To resolve the incompatibility, you must complete the following steps:

1. On any of the Switches listed, you must disable TCMP on a trunk (aggregated link) that connects to a Switch, as TCMP is not supported on the Switch.

2. You must disable auto-negotiation on all ports on the Switch that you want to place in an aggregated link before you place them in the aggregated link.

Refer to the Documentation on the Switch CD-ROM or the 3Com Web site for more information about

configuring aggregated links.

An incompatibility exists when changing link speed from 10 Mbps Half Duplex to 100 Mbps half duplex. If auto-negotiation on the Switch is disabled and the link speed on the Switch is changed from 10 Mbps half duplex to 100 Mbps half duplex, there is a possibility that the link partner will not detect the change. The link will have to be broken and reconnected before the link partner will detect the speed and change link speed to 100 Mbps half duplex.

Although it is possible to set up a slip connection from a PC running Windows 2000 to the console port of the switch using the *"Communications Cable between 2 computers"* modem type, the resulting setup only works intermittently.

Software Upgrades

How do I upgrade the Software on my Switch?

To upgrade the software on the Switch do the following:

1. Locate the upgrade software for the Switch and run the (*filename*.exe) executable file.
2. If necessary, download the TFTP server applications into the management station.
3. Install the TFTP server (file name *3ts01_04.exe*) on a Microsoft Windows 95, 98, NT or 2000 machine.
4. Launch the TFTP server application.
5. Point the Upload/Download default directory on the TFTP server to the directory where the upgrade file is located.
6. Make sure the Switch being upgraded has an IP address assigned to it.
7. Telnet to the Switch.
   a. To Telnet to the Switch, click Start in Microsoft Windows 95, 98, NT or 2000 machine.
   b. Click *Run*.
   c. In the text area, type **`telnet`** ***`IP address`***.
   d. Click *OK*.
8. Press *Enter* to receive a login prompt.
9. Log into the Switch management.
   a. The default user login is *admin*.
   b. There is no default password for admin (press *Enter*).
10. From the main menu, select *System*, then select *Control*.
11. Select *SoftwareUpgrade*.
12. Enter the IP address of the TFTP server connected to the Switch.
13. Enter the upgrade file name.
    a. This message will appear "Software upgrade in progress..."
    b. The entire time the upgrade is in process, the Power/Self test LED will flash ON/OFF Green, and a series of dots will indicate that the upgrade is progressing successfully
    c. When the software upgrade is complete, the Switch will reboot itself

3Com Network Supervisor

The CD-ROM contains 3Com Network Supervisor.

3Com Network Supervisor provides powerful yet easy-to-use network management. Focused on the needs of small to medium enterprises, it enables you to manage your network more efficiently. For larger networks (up to 2,500 nodes) and extra functionality you can purchase the 3Com Network Supervisor Advanced

Package.

To download the latest 3Com Network Supervisor and Service Pack please visit:

http://www.3com.com/3ns/

For HP OpenView users the 3Com Switch 4050 and 4060 (and all other 3Com managed products) are fully supported by the 3Com Integration Kit for HP OpenView (3C15300).

Documentation Errors and Omissions

Management Interface Reference Guide (DHA1770-9AAA03):

The **`protocol ip interface summary`** Command Line Interface (CLI) reference page should detail that the screen displays how the the IP interface was configured. For example, `"The IP address for interface 1 has been configured manually."`

The protocol ip interface summary CLI reference page contains the following statement:
“1. At the top-level menu, enter:
`protocol ip arp summary`”
This is incorrect. The statement should read:
“1. At the top-level menu, enter:
`protocol ip interface summary`”

The first information note on the **`protocol ip udpHelper add`** Command Line Interface (CLI) reference page should read as follows, if you have Version 3.05 software installed:

A maximum of 32 port/destination address pairs can be defined. A single UDP port can have up to 32 destination addresses configured against it. If a UDP port has multiple destination addresses, the packets are relayed to all of the addresses.

3Com Switch 4050 and 4060 Getting Started Guide (DUA1770-9AAA04)

Page 20 contains a table showing the default settings for the Switch. The entry for the Link Aggregation Control Protocol (LACP) feature should read “Disabled per port”.

3Com Switch 4050 and 4060 Implementation Guide (DUA1770-9BAA03)

Page 138 "Recovering your XRN Network - Unit Failure": step 5 should read: "If any Switch features, for example, IGMP snooping or passwords are not set to default state then these should be reset after the new Distributed Fabric has been formed.

Copyright © 2003, 3Com Corporation. All rights reserved.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo and SuperStack are registered trademarks of 3Com Corporation. XRN is a trademark of 3Com Corporation.

Windows and Windows NT are registered trademarks of Microsoft Corporation. Netscape Communicator is a registered trademark of Netscape Communications. Other brand and product names may be registered trademarks or trademarks of their respective holders.

Part No. DNA1770-9AAA04

Published April 2003